UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,524	11/01/2001	Ari D. Kaplan	2222.4350002	9108

26111 7590 06/18/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
06/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/040,524	KAPLAN, ARI D.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29,31-39 and 41-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29, 31-39, and 41-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 27, 2007 has been entered.

2. Claims 29, 31-39, and 41-48 are currently pending consideration.

Response to Arguments

3. Applicant's arguments with respect to claims 29, 31-39, and 41-48 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 29, 31-34, 37-39, 41-44, and 47-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneider et al. (U.S. Patent 6,178,505) in view of Carini et al. (U.S. Patent 6,636,873).

Regarding claim 29, Schneider discloses:

A wireless database management system, comprising:

a first server (Figure 1, item 107a) providing a first virtual private network (VPN) and providing Internet access (Figure 1, item 111) to user-held wireless communication devices (Figure 2, "clients") operating within an intranet environment (Figure 2, "the cluster of clients and servers isolated by each access filter is an intranet"), the VPN limiting access to a subset of the wireless communication devices that subscribe to the VPN (Figure 2, column 7, line 59 – column 8, line 15), *wherein each internal network (intranet) makes up a VPN which spans over the Internet, and access to each internal network comprising clients (user-held communication devices) is controlled by access filters (servers)* (column 8, lines 7-15);

a second server (Figure 1, item 107b) providing a second VPN with access to the Internet (Figure 1, item 111) providing access to one or more databases (Figure 1, item 115) associated with the subscribing subset of wireless communication devices (column 12, lines 53-60), *wherein an information resource (database) is associated with various user groups (subset of subscribing devices), wherein the information resource (database) is protected by another access filter (second server)*;

wherein operation of the first VPN and second VPN creates a VPN tunnel in the Internet restricted to data address to or from the subscribing subset of wireless communication devices (Figure 1, item 112, column 17, lines 45-53), *wherein a tunnel is created between the client (subscribing set of communication devices) and the information resource (database).*

Schneider does not explicitly disclose that the user-held wireless communication devices operating within the intranet environment include at least one of a personal digital assistant (PDA), cell phone, two-way pager or other mobile, hand-held, personal communication device. Carini discloses a system wherein mobile devices (Carini: Figure 4, item 414, column 8, lines 11-15) communicate with a mobile gateway server, possibly by use of a VPN (Carini: column 5, lines 64-67), to communicate with a replication database (Carini: column 8, lines 29-31). Schneider and Carini are analogous arts because both disclose systems wherein clients use a server (Schneider: "access filter", Carini: "mobile device gateway server") to communicate via a VPN to a remote database. The mobile devices of Carini can be implemented as the "clients" (Schneider: Figure 2) in Schneider wherein the access filter of Schneider provides the same functionality (limiting access, retrieving data from a database) of the mobile gateway server of Carini. It would have been obvious to one of ordinary skill in the art at the time of invention to use the mobile devices of Carini in the system of Schneider, because "the need to physically connect the computers 110, 112, 114, 116 to the network 118 through the LAN or a Wide Area Network (WAN 122 limits...mobility and

ability to dynamically respond to changing conditions" (Carini: column 1, lines 47-52). Therefore, using the mobile clients of Carini in the system of Schneider would allow for more mobility and flexibility of the clients (Schneider: Figure 2) of Schneider.

Claim 31 is rejected as applied above in rejecting claim 29. Furthermore, Schneider discloses:

The wireless database management system of claim 29 wherein the first virtual private network (VPN) operating on the first server providing Internet access to user-held wireless communication devices is a VPN-controlled wireless proxy server securing data transferred between the user-held wireless communication devices and the Internet (column 3, lines 58-63, column 15, lines 52-61), *wherein the access filter (server) contains a proxy which performs authentication and access checking, and also provides access to the Internet (Figure 1, item 111) and is connected to a VPN tunnel (Figure 1, item 112).*

Claim 32 is rejected as applied above in rejecting claim 29. Furthermore, Schneider discloses:

The wireless database management system of claim 29, wherein the data transfers between the server providing Internet access to user-held wireless communication devices are encrypted with a public key method (column 9, lines 47-53, column 10, lines 29-55), *wherein the database access request from the client is*

encrypted using a particular encryption technique, which can use Simple Key Management for Internet Protocols (SKIP) which manages public key exchange.

Claim 33 is rejected as applied above in rejecting claim 29. Furthermore, Schneider discloses:

The wireless database management system of claim 29, wherein the data transfers between the second server with access to the Internet and providing access to one or more databases associated with the subscribing set of wireless communication devices are encrypted with a private key method (column 17, lines 36-39), *wherein the database (information server) encrypts the information with the key for the access filter (second server).*

Claim 34 is rejected as applied above in rejecting claim 29. Furthermore, Schneider discloses:

The wireless database management system of claim 29, wherein users of the wireless communication devices are authenticated before allowing access to the databases (column 10, lines 29-36), *wherein the users are authenticated using certificates, authentication tokens, and/or IP address/domain names.*

Claim 37 is rejected as applied above in rejecting claim 29. Furthermore, Schneider discloses:

The wireless database management system of claim 29, wherein a firewall (Figure 1, item 109a) is implemented between the Internet (Figure 1, item 111) and the second server (Figure 1, item 113) connected to the databases, thereby limiting access to IP addresses of the wireless communication devices (Figure 1, item 109a, column 4, lines 21-34), *whereby the access filter checks IP addresses of incoming packets before forwarding the packets to the clients.*

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, Schneider discloses:

The wireless database management system of claim 37, wherein a second firewall is implemented between the second server and the databases (Figure 1, item 109b, column 2, lines 48-54), *wherein the firewall is implemented between the access filter (second server) and the database in order to protect the internal network containing the database.*

Regarding claim 39, Schneider discloses:

A method for securing data in a wireless database management system, comprising the steps of:

a) providing a first server (Figure 1, item 107a) including a virtual private network (VPN) and providing Internet access (Figure 1, item 111) to user-held wireless communication devices (Figure 2, "clients") operating within an intranet environment (Figure 2, "the cluster of clients and servers isolated by each access filter is an

intranet"), the VPN limiting access to a subset of the wireless communication devices that subscribe to the VPN (Figure 2, column 7, line 59 – column 8, line 15), *wherein each internal network (intranet) makes up a VPN which spans over the Internet, and access to each internal network comprising clients (user-held communication devices) is controlled by access filters (servers)* (column 8, lines 7-15);

b) providing a second server (Figure 1, item 107b) including a VPN with access to the Internet (Figure 1, item 111) and providing access to one or more databases associated with the subscribing set of wireless communication devices (column 12, lines 53-60), *wherein an information resource (database) is associated with various user groups (subset of subscribing devices), wherein the information resource (database) is protected by another access filter (second server)*;

c) operating the first and second server VPNs to create a VPN tunnel in the Internet restricted to data addressed to or from the subscribing subset of wireless communication devices (Figure 1, item 112, column 17, lines 45-53), *wherein a tunnel is created between the client (subscribing set of communication devices) and the information resource (database)*.

Schneider does not explicitly disclose that the user-held wireless communication devices operating within the intranet environment include at least one of a personal digital assistant (PDA), cell phone, two-way pager or other mobile, hand-held, personal communication device. Carini discloses a system wherein mobile devices (Carini: Figure 4, item 414, column 8, lines 11-15) communicate with a mobile gateway server,

possibly by use of a VPN (Carini: column 5, lines 64-67), to communicate with a replication database (Carini: column 8, lines 29-31). Schneider and Carini are analogous arts because both disclose systems wherein clients use a server (Schneider: "access filter", Carini: "mobile device gateway server") to communicate via a VPN to a remote database. The mobile devices of Carini can be implemented as the "clients" (Schneider: Figure 2) in Schneider wherein the access filter of Schneider provides the same functionality (limiting access, retrieving data from a database) of the mobile gateway server of Carini. It would have been obvious to one of ordinary skill in the art at the time of invention to use the mobile devices of Carini in the system of Schneider, because "the need to physically connect the computers 110, 112, 114, 116 to the network 118 through the LAN or a Wide Area Network (WAN 122 limits...mobility and ability to dynamically respond to changing conditions" (Carini: column 1, lines 47-52). Therefore, using the mobile clients of Carini in the system of Schneider would allow for more mobility and flexibility of the clients (Schneider: Figure 2) of Schneider.

Claim 41 is rejected as applied above in rejecting claim 39. Furthermore, Schneider discloses:

The method of claim 39 wherein in step a), the first server providing access to user-held wireless communication devices is a VPN-controlled wireless proxy server securing data transferred between the user-held wireless communication devices and the Internet (column 3, lines 58-63, column 15, lines 52-61), *wherein the access filter (server) contains a proxy which performs authentication and access checking, and also*

provides access to the Internet (Figure 1, item 111) and is connected to a VPN tunnel (Figure 1, item 112).

Claim 42 is rejected as applied above in rejecting claim 39. Furthermore, Schneider discloses:

The method of claim 39 wherein in step a) the data transfers between the first server providing Internet access to user-held wireless communication devices are encrypted with a public key method (column 9, lines 47-53, column 10, lines 29-55), *wherein the database access request from the client is encrypted using a particular encryption technique, which can use Simple Key Management for Internet Protocols (SKIP) which manages public key exchange.*

Claim 43 is rejected as applied above in rejecting claim 39. Furthermore, Schneider discloses:

The method of claim 39 wherein in step b) the data transfers between the second server with access to the Internet and providing access to one or more database associated with the subscribing subset of wireless communication devices are encrypted with a private key method (column 17, lines 36-39), *wherein the database (information server) encrypts the information with the key for the access filter (second server).*

Claim 44 is rejected as applied above in rejecting claim 39. Furthermore, Schneider discloses:

The method of claim 39, further providing a step of authenticating users of the wireless communication devices before allowing access to the databases (column 10, lines 29-36), *wherein the users are authenticated using certificates, authentication tokens, and/or IP address/domain names.*

Claim 47 is rejected as applied above in rejecting claim 39. Furthermore, Schneider discloses:

The method of claim 39 wherein in step b) a firewall (Figure 1, item 109a) is provided between the Internet (Figure 1, item 111) and the second server (Figure 1, item 113) connected to the databases, thereby limiting access to IP addresses of the wireless communication devices (Figure 1, item 109a, column 4, lines 21-34), *whereby the access filter checks IP addresses of incoming packets before forwarding the packets to the clients.*

Claim 48 is rejected as applied above in rejecting claim 47. Furthermore, Schneider discloses:

The method of claim 47 wherein a second firewall is implemented between the second server and the databases (Figure 1, item 109b, column 2, lines 48-54), *wherein the firewall is implemented between the access filter (second server) and the database in order to protect the internal network containing the database.*

5. Claims 35-36 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneider et al. (U.S. Patent 6,178,505) in view of Carini et al. (U.S. Patent 6,636,873) in further in view of Ludovici et al. (U.S. Patent 6,636,898).

Claim 35 is rejected as applied above in rejecting claim 29. The system of Schneider and Carini does not explicitly disclose setting an adjustable timeout for connections between the wireless communication devices and the server. The system of Schneider and Carini provides wireless communication devices communicating with a server (access filter in Schneider) using VPN (encrypted tunnel). Ludovici discloses a system that controls connections to a VPN manually by setting timeouts on VPN connections by using a VPN manager (Ludovici: column 3, lines 48-57). Ludovici is an analogous art to Schneider and Carini, as in all three references use VPNs a secure mode of communication. Ludovici uses the adjustable timeouts of these VPN connections in for the purpose of "limiting these VPN connections to a particular lifetime" (Ludovici: column 10, lines 57-60) and for "security reasons and connection manageability reasons" (column 1, lines 57-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the adjustable timeout of Ludovici in the system of Schneider-Carini in order to limit the lifetime of the VPN connections to insure that the VPN connection is not compromised (Ludovici: column 1, lines 60-61).

Claim 36 is rejected as applied above in rejecting claim 35. Schneider and Carini do not explicitly state identifying a session between the wireless communication device and the second server with a session identification phrase and storing that phrase in memory. . The system of Schneider and Carini provides wireless communication devices communicating with a server (access filter in Schneider) using VPN (encrypted tunnel). Ludovici discloses a system that controls connections to a VPN manually by setting timeouts on VPN connections by using a VPN manager (Ludovici: column 3, lines 48-57), and these connections (sessions) are identified by a connection name (Ludovici: Figure 11, item 260) which contain a connection definition (Ludovici: Figure 12, item 26). This connection definition (session ID) is a database entry which defines all attributes of the connection (Ludovici: column 8, lines 7-10). The connection (session ID) name is needed so that the VPN manager can keep track of the lifetimes of different connections and initiate timeouts and/or other actions on the different connections (sessions) (Ludovici: column 3, lines 48-57). Ludovici is an analogous art to Schneider and Carini, as in all three references use VPNs a secure mode of communication. Ludovici uses the adjustable timeouts of these VPN connections in for the purpose of "limiting these VPN connections to a particular lifetime" (Ludovici: column 10, lines 57-60) and for "security reasons and connection manageability reasons" (column 1, lines 57-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the adjustable timeout of Ludovici in the system of Schneider-Carini in order to limit the lifetime of the VPN connections to insure that the VPN connection is not compromised (Ludovici: column 1, lines 60-61).

Claim 45 is rejected as applied above in rejecting claim 39. The method of Schneider and Carini does not explicitly disclose setting an adjustable timeout for connections between the wireless communication devices and the server. The method of Schneider and Carini provides wireless communication devices communicating with a server (access filter in Schneider) using VPN (encrypted tunnel). Ludovici discloses a method that controls connections to a VPN manually by setting timeouts on VPN connections by using a VPN manager (Ludovici: column 3, lines 48-57). Ludovici is an analogous art to Schneider and Carini, as in all three references use VPNs a secure mode of communication. Ludovici uses the adjustable timeouts of these VPN connections in for the purpose of "limiting these VPN connections to a particular lifetime" (Ludovici: column 10, lines 57-60) and for "security reasons and connection manageability reasons" (column 1, lines 57-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the adjustable timeout of Ludovici in the system of Schneider-Carini in order to limit the lifetime of the VPN connections to insure that the VPN connection is not compromised (Ludovici: column 1, lines 60-61).

Claim 46 is rejected as applied above in rejecting claim 39. Schneider and Carini do not explicitly state identifying a session between the wireless communication device and the second server with a session identification phrase and storing that phrase in memory. . The system of Schneider and Carini provides wireless communication devices communicating with a server (access filter in Schneider) using VPN (encrypted tunnel).

Ludovici discloses a system that controls connections to a VPN manually by setting timeouts on VPN connections by using a VPN manager (Ludovici: column 3, lines 48-57), and these connections (sessions) are identified by a connection name (Ludovici: Figure 11, item 260) which contain a connection definition (Ludovici: Figure 12, item 26). This connection definition (session ID) is a database entry which defines all attributes of the connection (Ludovici: column 8, lines 7-10). The connection (session ID) name is needed so that the VPN manager can keep track of the lifetimes of different connections and initiate timeouts and/or other actions on the different connections (sessions) (Ludovici: column 3, lines 48-57). Ludovici is an analogous art to Schneider and Carini, as in all three references use VPNs a secure mode of communication. Ludovici uses the adjustable timeouts of these VPN connections in for the purpose of "limiting these VPN connections to a particular lifetime" (Ludovici: column 10, lines 57-60) and for "security reasons and connection manageability reasons" (column 1, lines 57-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the adjustable timeout of Ludovici in the system of Schneider-Carini in order to limit the lifetime of the VPN connections to insure that the VPN connection is not compromised (Ludovici: column 1, lines 60-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kaveh Abrishamkar 6/11/07

Kaveh Abrishamkar
AU 2131

KA 6/11/07
KA
06/11/2007